REMARKS

Pending Claims:

Claims 1 to 8 and 10 to 16 are pending in this application. Claim 9 is cancelled, without prejudice. The subject-matter of claim 9 has been incorporated into claim 8. Claims 1, 8, 13, 15 and 16 have been amended to further define and describe the invention. No new matter has been added by way of these amendments. Reconsideration is respectfully requested in view of the amendments and the remarks herein.

Rejections of the Claims:

Claims 1 to 3, 8 to 9 and 13 are rejected under 35 U.S.C. 102(e) as being unpatentable by Mizikovsky (U.S. 2001 0044296). Claims 4 to 7, 10 to 12 and 14 to 16 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Mizikovsky and further in view of Ritter (U.S. 6543686).

Mizikovsky discloses a telecommunications system in which a mobile terminal may have its "parameters" updated over-the-air. The parameters may, for example, be the radio frequencies that the mobile terminal should use under a given circumstance (see paragraph 0006). An arrangement is described by which the parameters of a mobile terminal 404 can be updated wirelessly by an over-the-air functional entity 402. In particular, an arrangement is described whereby such updating can be performed even when the mobile terminal 404 is not in its home telecommunications network 401, but is in a visited or serving wireless telecommunications network 403.

With reference to Figure 5 of Mizikovsky, the over-the-air procedure involves the following series of steps. At **step 501**, the over-the-air functional entity 402 transmits an enquiry to the home telecommunications network 401 of the terminal 404 to determine by which network the terminal 404 is currently being served. At **step 502**, the home network 401 transmits to the over-the-air functional entity 402 an identifier of the relevant network (in the embodiment the serving network 403 - as the terminal 404 is "roaming" in that network). At step **503**, the over-the-air functional entity 402 transmits a request to update at least one parameter in the terminal 403 to the serving network 403. At **step 504,** the serving network 403 delivers this request to the terminal 404.

So as not to allow an unauthorized third party to update the parameters of the terminal 404, an authentication process is then performed in which the legitimacy of the over-the-air functional entity 402 is verified to the terminal 404 (that is, the <u>terminal</u> 404 authenticates the over-the-air functional entity 402).

To this end, at **step 505**, terminal 404 generates and sends an authentication challenge, x, to the serving network 403. At **step 506**, the serving network 403 transmits this challenge, x, to the over-the-air functional entity 402. The over-the-air functional entity 402 does not have secret value, s, and it is not therefore able to generate an appropriate response to the challenge, x. Only the home network 401 knows the secret value, s. Therefore, at **step 507**, the over-the-air functional entity 402 forwards the authentication challenge, x, to the authentication center in the home network 401.

The authentication center retrieves the secret value, s, and evaluates the function $f(s,x)$ based on the authentication challenge, x, and the secret value, s, to generate an authentication response, r. The authentication response, r, serves as the credential that the over-the-air functional entity 402 will use to evidence its authenticity to wireless terminal 404. At **step 508**, the home network 401 transmits the authentication response, r, to the over-the-air functional entity 402. At **step 509**, the over-the-air functional entity 402 forwards the authentication response, r, to the serving network 403. At **step 501**, the serving network 403 delivers the authentication response, r to the mobile terminal 404.

The mobile terminal 404 compares the received authentication response, r, to the expected value that it has itself calculated using the values of x and s known to it. If the two values match, then the terminal 404 concludes that the over-the-air functional entity 402 is not an imposter and is authorized to provide it with new parameters. Accordingly at **step 511**, terminal 404 transmits a validation response to the serving network 403. This is delivered to the over-the-air functional entity 402 at **step 512**. At **step 513**, the over-the-air functional entity 402 transmits at least one parameter to the serving network 403 for delivery to the wireless terminal 404 at **step 514**. When the over-the-air functional entity 402 has finished transmitting the parameters to the terminal 404, the over-the-air functional entity 402 transmits a termination message to the terminal 404 which directs the terminal 404 not to accept any new parameters without again going through steps 505 to 511, described above. The termination messages are transmitted by the over-the-air functional entity 402 to the serving network 403 at **step 515**, and from the serving network 403 to the terminal 404 at **step 516**.

As discussed above, Mizikovsky describes a system in which a roaming mobile terminal can authenticate a device wishing to perform an over-the-air update of its functional parameters. Mizikovsky does not relate at all to an arrangement for allowing a home mobile telecommunications network to authenticate a mobile terminal located in an area served by a serving mobile telecommunications network so that the mobile terminal may make and receive telephone calls (as taught by the application).

Claims 1,8 and 13 have been amended to emphasize that the home mobile telecommunications network is operable to generate authentication vectors for enabling the mobile terminal to obtain an <u>identifier</u> (having a value) from the serving mobile telecommunications network, which identifier is transmitted from the mobile terminal to the serving network to allow the terminal to make calls within the serving network. _(See, e.g.,_ claim 1, "the home mobile telecommunications network is operable to generate authentication vectors for enabling the mobile user equipment to obtain an identifier having a value from the serving network, which identifier is transmitted from the mobile user entity to the serving network to allow the mobile user equipment to make calls by wireless communication between the mobile user equipment and the serving mobile telecommunications network when within the area covered by the serving mobile telecommunications network".) An authentication element forming at least part of the authentication vector is passed from the serving network to the mobile terminal. The mobile terminal then decides, based at least in part on the value of a predetermined field contained in the authentication element, when to generate a termination message. The termination message, when generated, is passed from the mobile terminal to the serving network. Importantly, this message comprises the <u>identifier,</u> but with a value different from the aforementioned value, and which value indicates that the serving network must obtain further authentication vector from the home network before allowing the user equipment to make further calls within the serving network.

In the embodiments described in the present specification, the claimed "identifier" is a Key Set Identifier (KSI). The transmission of such a KSI from a serving mobile network to a mobile terminal, and subsequently from the mobile terminal to the serving network each time that terminal wishes to make a call using the serving network, occurs as a matter of course according to the mobile telecommunications standards described in the present specification. In accordance with the present specification, the mobile terminal causes the serving network to obtain a new authentication vector from the home network by changing the value of the KSI. The mobile terminal must therefore be authenticated with its home network before making further calls within the serving network. The home network will not generate an authentication vector if it does not wish the mobile terminal to make further calls - for example, because that mobile terminal has exceeded its call limit.

It is highly significant that the serving network can be caused to force re-authentication of the roaming mobile terminal with the home network <u>without changing the signaling structure between the various components of a telecommunications system comprising the home network, the serving network, and the mobile terminal</u>. As discussed

above, the signaling structure is highly standardized and cannot be readily changed. The present invention advantageously allows the existing signaling structure to provide additional functionality. Such an advantageous arrangement is not disclosed or suggested at all by Mizikovsky. It is therefore respectfully submitted that the amended claims are neither anticipated nor rendered obvious by Mizikovsky.

Dependent claims 4 to 7, 10 to 12 and 14 to 16 are rejected as being obvious over Mizikovsky in view of Ritter. This rejection is respectfully traversed on the following grounds. Firstly, each of the dependent claims is submitted to be allowable because it is dependent, either directly or indirectly, upon an allowable main claim. Secondly, Ritter has a U.S. filing date after the priority date of the present application and cannot therefore be properly cited.

Conclusion:

The application is considered to be in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,
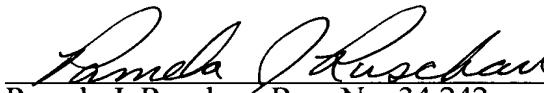
Pamela J. Ruschau, Reg. No. 34,242
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson Avenue
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: January 4, 2005

Amendment or ROA - Final (Revised 7/29/03)